SHRM®
BETTER WORKPLACES
BETTER WORLD™

How to Protect Company Data When Laying Off Remote Workers

By Roy Maurer
May 20, 2020

Laying off employees is always painful, but having to do so when they are completely remote adds a new wrinkle: What should employers do to protect the company's data on laptops and other devices when letting remote workers go?

continued next page

Brian Schrader, president and CEO of BIA, an electronic discovery and digital forensics firm in New York City, spoke with SHRM Online about this tricky subject.

SHRM Online: What are the steps employers should take to protect company data when laying off remote employees?

Schrader: The first step begins before the employee leaves. The company should have in place clear policies that outline what data the organization owns and the ways it protects and secures that data. To ensure that employees are aware of those policies and their role in protecting company data generally, you should have each employee sign an agreement, preferably when hired, that lays out the organization's data-security practices and policies, as well as what the company expects of the employees themselves. The agreement should make clear that company data cannot be taken or shared during employment or upon an employee's departure, and also that the company has the right to monitor and wipe any personal devices of company data.

Even if those policies were not previously in place, you can require that the employee sign an agreement upon departure that states data has not been taken from the company, and all company-owned devices have been returned as part of the exiting-employee process. Use a questionnaire or exit interview to ask the employee where they may have stored company data to ensure you have all of it identified and remediated. You can use the same process to gather any passwords that the employee may have used for encrypted files and systems, as well as any third-party services that may have been used for business purposes, even if not officially approved, where company data may reside.

At or before the time of exit, make sure to disable the employee's accounts and access to all company-owned systems, equipment and company-managed third-party resources, whether the worker is working from home or in the office. The employee should no longer be able to view or work with company files, e-mail, software or online platforms. Physical access should be removed, as well, meaning the employee should return any keys, fobs, parking passes, etc. Any company equipment, including laptops, external hard drives and thumb drives, should be returned to the office on the last day or shipped back. Additionally, any company data that may be on the employee's personal devices, such as a smartphone or tablet, should be wiped. Most mobile-device management systems can target data to ensure that only company data, not personal information, is removed.

continued next page

SHRM Online: What's the best practice regarding return of hardware such as laptops and company smartphones and tablets during this lockdown period?

Schrader: Send a flat shipping box, packing materials and a prepaid shipping label to the employee. That makes it easier for them to send things back immediately. Make them aware that the ship date should be the person's last day or whatever date is determined by the company.

Once the devices are returned, hold them for at least 90 days before reissuing them to another user. This gives you time to determine if you need to forensically image the data for any legal or investigative use later. Typically, any employee theft or other issue will show itself within a few months. Plus, the hold period helps you know that you haven't lost any needed data due to a company device being wiped prematurely. In the case of extremely sensitive employees like senior executives, high-performing salespeople and the like, you may want to forensically image the devices before reissuing them after that 90-day period, regardless of whether or not you have a known issue, just as an extra precaution.

SHRM Online: What are the legal considerations around employee data on company-owned devices?

Schrader: While the European Union and other jurisdictions have significantly more restrictive and punitive personal-data privacy laws, in the United States, the employee generally has no privacy right to data they put on a company-owned system. That said, best practice would be to instruct the employee to remove any personal information on company-owned devices before the employee leaves. There also should be verbiage in the company's data policies and exiting-employee agreements that states that any personal data left with the company upon departure becomes the property of the company and can be destroyed at the company's discretion.

If the company is ever involved in a legal matter, it's possible that the employee's data could be collected as part of discovery. While not required, to be extra careful, the employee agreement could include a statement noting that the company is not responsible for any consequences of the employee's personal data being on any company-owned devices. That way, if it's ever mixed into such a discovery effort, the company can't be held responsible for any disclosure or misuse of that data.

SHRM Online: What kind of activity would warrant a forensic audit?

Schrader: A forensic audit is warranted if there is any suspicion of data theft [or there are] harassment claims, criminal conduct or other suspected or known inappropriate acts or behavior by the employee prior to departure. In other words, if there is any

continued next page

reason to investigate a given employee's actions—as opposed to gathering data for just general legal discovery or regulatory purposes, for example—then a forensic investigation may be appropriate.

At that point, the employee's former devices and any other digital resources should be preserved beyond the initial 90-day hold period. It's crucial that the devices and data are not accessed by anyone without computer forensic training, as even well-meaning IT professionals could accidentally alter or destroy critical information. During a forensic audit, the data is forensically collected, which generally means it is imaged or otherwise collected in a way that maintains original metadata, log and system files, unallocated and free space where deleted items may still reside, and other critical information.

SHRM Online: What can a digital forensic audit uncover?

Schrader: A digital forensic investigation involves looking at all the data collected to determine if there are any indications of wrongdoing. Forensic experts analyze files, including deleted documents and system information, as well as system logs and other information. They will flag potential bad behavior, including:

- If confidential files or large amounts of data were transferred to noncompany external devices, like USB drives, or online repositories like Box or Google Drive.
- If data usage and transfers increased in the few days before the employee left or took place outside of regular business hours.
- If software was recently added to or removed from a company-owned device, especially if there do not seem to be many related files for that system.
- If a personal Web mail, online repository or similar account was logged into from any of the employee's devices.
- If the user accessed company data sources that were not within their job description and/or inconsistent with company policy.
- Evidence of any bulk deletion of data from the devices prior to exit.

As the investigation proceeds, the forensic investigator will also attempt to recover any deleted, lost or compromised data, review system and user log files for unusual activity, and much more. The results may then lead to legal claims and other ramifications.

Seventy-two percent of employees think the data they create and manage on the job belongs to them. We have found that, if there is evidence of employee data theft, the best course of action is to address it directly with the employee. Typically, when the employee is found out, they will return or delete the stolen files, most often not realizing they had broken a company policy. If that doesn't work though, these processes ensure your company will be prepared for litigation.